AN ON-LINE FAULT TREE ANALYSIS FOR THE CONTINUOUS MONITORING OF INDUSTRIAL PLANT ACCIDENTS

Compagno, L. 1, D'Urso, D. 1, Maiolino, L. 2, Nicotra, V. 3, Spampinato, S. 4, Trapani, N. 1
1 D.I.I.M., University of Catania, viale A. Doria 6, Catania, 95125 Italy
2 Isab Energy Services, Priolo Gargallo (SR), Italy
3 Blue Consulting s.r.l.
4 Erg S.p.A.

ABSTRACT

The Seveso Directive states that if a plant is subject to relevant accident risks it is necessary that the Plant Manager edits a Safety Report through which he can show that a risk analysis was executed in order to assess the risk related to the use of dangerous substances. There are a lot of well known techniques for executing the risk analysis of a process plant but only a few of these are quantitative, such as Fault Tree Analysis (FTA) that allows to assess the occurrence of a potential major event (Top Event). An On-line Fault Tree Analysis (OLFTA) was developed which, interfaced with the Distributed Control System of the plant, is able to assess the probability of the top event, taking into account of unavailable equipment, for failure or maintenance causes.

1.0 INTRODUCTION

The D.Lgs 238/2005 [1], which has modified in Italy the D.Lgs 334/99 [2], transposition of Council Directive on the control of major-accident hazards involving dangerous substances (Seveso II [3]), states that if a plant is subjected to a relevant accident hazard it is necessary that the Plant Manager edits a Safety Report through which he can show that a risk analysis was executed in order to assess the hazards related to the use of dangerous substances. The applicative decrees of these laws suggest some qualitative methodologies in order to identify risks, such as FMEA (Failure Mode and Effect Analysis) or HAZOP (Hazard and Operability Studies), and some quantitative ones, such as FTA (Fault Tree Analysis) and ETA (Event Tree Analysis) in order to assess the risk level.

In a plant subjected to major-accident hazard, an HAZOP analysis can be carried out not only to satisfy law requirements, but also in order to obtain:

- a deep knowledge of plant functioning;
- an hard reduction of costs related to unpredictable failure of plant;
- an evidence of environmental compatibility of the plant.

FTA is a well known technique for reliability and safety analysis, used in industrial plants to point out how logical relationship between equipment failures, human errors and external events can combine each other to cause specific accidents, explosion, toxic release. FTA allows to determine the probability of system failure and its reliability/availability, the expected number of failure in a period, the rate of failure of the system, and other reliability parameters. FTA method analysts apply a top-down logic in building models, starting from a top event (TE), which can be a relevant failure or accident, through intermediate events and stopping when they have identified the basic faults (primary causes) that led to TE. The basic failure events are the ones for which it is possible to assign failure rates. The failure rate data have usually a statistical origin and they can be taken from a variety of sources, such as industry or equipment

manufacturer historical databases. The data coming from equipment manufacturers are considered more credible but they are often unavailable; the data registered by the equipment end-user (the plant manager) can also be very significant, but often their contents are incomplete or useless.

Such analysis gives "ideal" results which are significant only for process and plant design phase, but during normal operative life a lot of events can occur, such as equipment failures or preventive maintenance activities, that can vary the project configuration and then the plant instantaneous availability/reliability.

Dynamic fault tree methodologies were defined in the past for computer systems [4, 5] and to improve safety of nuclear power plants [6] but rarely they are widespread used [7], also because of the gap between the modelled system and the real one [8].

A new technique is proposed in order to realize an instantaneous FTA (OLFTA) and we tested it in a power production plant. The difference between analyses already proposed and OLFTA methodology is the possibility to interact with the control system of the plant, in order to be able to underline the state of the equipment really involved in the analysis and to evaluate faults and lack of safety. The system, that is both simple and robust, allows to the Plant Manager to be continuously informed about the actual risk level of its installations, in order to make more correct operative choices. It also has the usability characteristics and reasonable costs which the industrial users requires.

2.0 PLANT DESCRIPTION

The Integrated Gasification Combined Cycle (IGCC) plant, placed in Priolo Gargallo (SR), is managed by ISAB Energy Services S.p.A. The gasification process treats high-sulfur coal, heavy petroleum sludge and biomasses in order to obtain Syngas, a clean fuel used for electric power generation.

The plant consists of the production units specified in Table 1.

Table 1. Plant unit description

Unit	Description
3000	Solvent deasphalting (SDA)
3100	Gasification unit
3200	Carbon recovery and recycle
3300	Syngas heat recovery-saturation and expansion
3400	Heavy metals recovery
3500	Acid gas removal unit
3600	Sulphur recovery
3700	Tail gas treatment
3900	Liquid sulphur storage and loading
4000	Combined cycle
4100	Electrical energy transformation & distribution
Utilities	Utilities plant

In order to facilitate the comprehension of the OLFTA technique, we will consider only a part of the plant, the unit 3200 "Carbon Recovery and recycle", which separates the soot contained in the soot water obtained by the Gasification unit in order to transform all the input carbon in gas. Before entering the decanter the soot water is partially depressurized and mixed with naphtha, in order to obtain a more effective separation of the soot inside the decanter. The water, heavier, comes out from the column bottom

and it is first sent to a gas-water separator; then it is divided into two stream: the most part is sent to the gasification unit as quench water; a little part is sent to the unit 3400 for heavy metal recovering.

The suspension of soot in the naphtha phase, lighter, comes out from the top of the decanter and it is mixed with the asphalt phase. The naphtha-asphalt-soot is subjected to a two phases preheating and it is sent to a stripping column in order to separate naphtha. The asphalt and the soot, which are less volatile, are pumped from the lower of the column to the gasification unit. Through a steam injection in the column, the naphtha is vaporized and then condensed in order to send it again to the decanter.

3.0 TOP EVENT IDENTIFICATION AND FAULT TREE CONSTRUCTION

The essential element to create a Fault Tree is the deep knowledge of the process, of the equipment and instrumentations operating in the plant and of their connections trough pipelines. For this reason, an accurate HAZOP analysis, executed by a team of instrumental, technology and safety engineers, allowed us to identify the causes of each potential accidental event, and to know all the safeguards acting in the plant. Such an analysis is an important starting point in order to identify all the concurrent events that can lead to a Top Event (TE); in the column "Note" of the HAZOP report the Top Event was explicitly indicated which the cause can contribute to.

In the unit 3200 "Carbon Recovery and Recycle" the five potential Top Events described in Table 2 have been identified.

Table 2. Unit 3200 Carbon Recovery and Recycle – Top Events

Top Event	Description
TE1	Very high pressure in D101 (liquid phase)
TE2	Very high pressure in D101 (very low level in R101)
TE3	Very high pressure in D102
TE4	Very high pressure in D104
TE5	Very high pressure in D105

The most critical event is TE2 "Very high pressure in D101 (very low level in R101)" as shown in Figure 1.

The Fault Tree of TE2 was realized using four simple logic gates, which are [9, 10]:

- AND-gate: the output event occurs if all of the input events occur;
- OR-gate: the output event occurs if at least one of the input events occur;
- SPARE-gate: the output event occurs if the number of spares is less than required (also k/m-gate);
- INHIBIT-gate: the output event occurs if the (single) input fault occurs in the presence of an enabling condition.

Other gates can be used for constructing fault trees, such as:

- PAND-gate (Priority AND): the output occurs only if all input events occur and in sequence from left to right;
- SEQ-gate (Sequence enforcing): the output event occurs only if input events occur in a particular order and there are more than two input events.

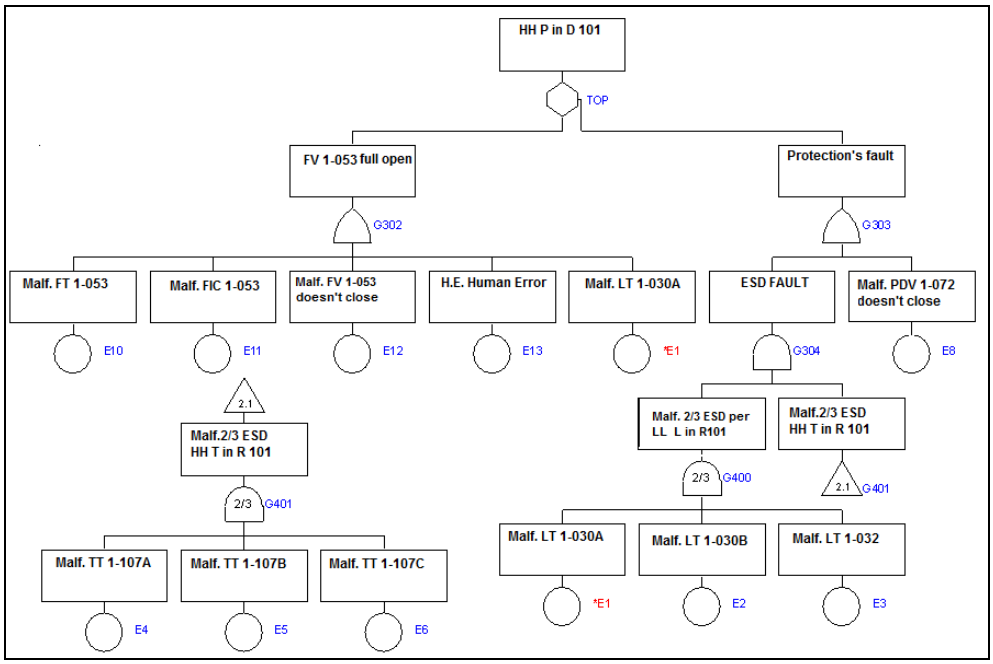

Figure 1. Fault tree of the TE2 "Very high pressure in D101 (very low level in R101)"

The causes of the event have been identified and an event's list was made in order to assess for each failure event (identified through Exx, in Table 3) the significant reliability parameters.

Table 3. Failure Events' List

Id	Event Code	Description
1	E10	FT 1-053 malfunctioning
2	E11	FIC 1-053 malfunctioning
3	E12	FV 1-053 malfunctioning (full open)
4	E13	H.E. – Hand Valve Open
5	E08	PDV 1-072 malfunctioning (doesn't close)
6	E04	TT 1-107A malfunctioning
7	E06	TT 1-107C malfunctioning
8	E05	TT 1-107B malfunctioning
9	E02	LT 1-030B malfunctioning
10	E01	LT 1-030A malfunctioning
11	E03	LT 1-032 malfunctioning

3.1 Equipment instantaneous unavailability calculation and relationship between equipment failures

In Table 4, a brief description of significant reliability data is reported, both for repairable and not repairable equipment, related to Basic Events (BE), Minimal Cut Sets (MCS) and Top Events (TE).

Table 4. Reliability parameters definitions for Fault Tree calculation

Name	Definition	BE	MCS	TE
Failure rate	The limit, if it exists, of the ratio of the conditional probability that the instant of time, T, of a failure of an item falls within a given time interval, $(t, t + \Delta t)$ and the length of this interval, Δt, when Δt tends to zero, given that the item is in an up state at the beginning of the time interval	λ	-	-
MTTR	Mean Time To Restoration	τ	-	-
PFD	Probability of Failure on Demand (for standby equipment or safety systems)	pfd	PFD	PFD_T
Mission time	Time interval during which we want the component to perform its required functions under stated conditions	t_M	t_M	t_M
Unreliability	Probability that there is a fault in the time interval $[0,t_M]$ (not repairable systems)	f	F	F_T
Reliability	Probability that there isn't a fault in the time interval $[0,t_M]$ (not repairable systems)	r	R	R_T
Steady State Unavailability	Probability that a component is in a failure state (repairable systems)	q	Q	Q_T
Instanteous Unavailability	Instantaneous probability that a component running at t=0 is in a failure state at time t (repairable systems)			
Availability	Instantaneous probability that a component running at t=0 is also running at time t (repairable systems)	a	A	A_T
Rate of Failure	Expected number of failures in a time unit (repairable systems)	rf	RF	RF_T
Expected Number of Failures	Expected number of failures in the time interval [0,t] (repairable systems)	enf	ENF	ENF_T

The relations between the reliability parameters of BE, MCS and TE are well established and known in literature [10, 11].

3.2 Equipment involved in potential accidental events identification

Table 5 shows the failure rates (λ), the test interval for the monitored equipment (T), and the mission time (t_M) for non repairable systems related to Basic Events of the Figure 1 Fault Tree.

Table 5. Failure Events reliability data (Mission time 8760 hours) (continued)

Id	Event Code	Event's List	λ [h^{-1}]	T [h]
1	E10	FT 1-053 malfunctioning	8,50E-06	-
2	E11	FIC 1-053 malfunctioning	4,80E-06	-
3	E12	FV 1-053 malfunctioning (full open)	1,64E-06	-
4	E13	H.E. – Hand Valve Open	5,70E-07	-
5	E08	PDV 1-072 malfunctioning (doesn't close)	1,64E-06	7,20E+02
6	E04	TT 1-107A malfunctioning	5,50E-06	1,68E+02
7	E06	TT 1-107C malfunctioning	5,50E-06	1,68E+02

Id	Event Code	Event's List	λ [h^{-1}]	T [h]
8	E05	TT 1-107B malfunctioning	5,50E-06	1,68E+02
9	E02	LT 1-030B malfunctioning	3,50E-06	1,68E+02
10	E01	LT 1-030A malfunctioning	3,50E-06	1,68E+02
11	E03	LT 1-032 malfunctioning	3,50E-06	1,68E+02

The failure rates shown in Table 5 were assessed through an historical analysis of each item operative life, which was possible by observing the Trend Control Graphics in the Plant Distributed Control System (DCS), as shown in Figure 2.

The manufacturer reliability data or literature data were used when operative data were not available for the item.

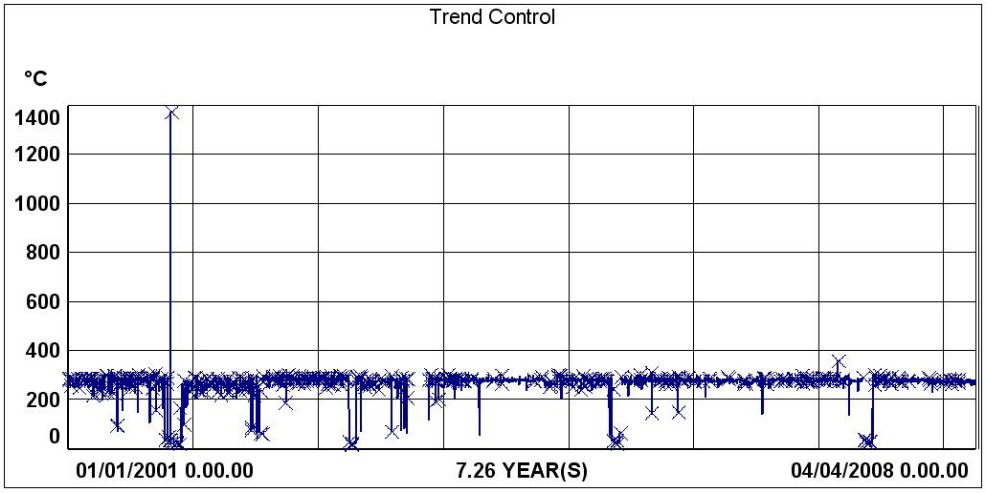

Figure 2. Trend Control Graphic of the TT-107A (setup value 274,0 °C)

4. ON-LINE FAULT TREE ANALYSIS (OLFTA)

A conventional FTA assumes that each system equipment works (with a given probability) during the instantaneous unavailability/reliability assessment. During the normal running of a plant one or more components can very often be out-of-service, therefore the overall unavailability of the Top Event is no longer equal to this evaluation. It is very important for plants safety to monitor how the instantaneous unavailability changes to activate action in order to avoid any accident.

OLFTA has this scope, it allows to know time by time what is the actual instantaneous unavailability of the Top Event and to warn the operator if the instantaneous unavailability is changing. To this extension OLFTA need to have data immediately available regarding the state of each component.

The industrial plant we considered is endowed with a data management system (DCS) which receives a signal from each equipment; in this way it is possible to know, in real time, the state of the equipment (running or in failure state, see Figure 3).

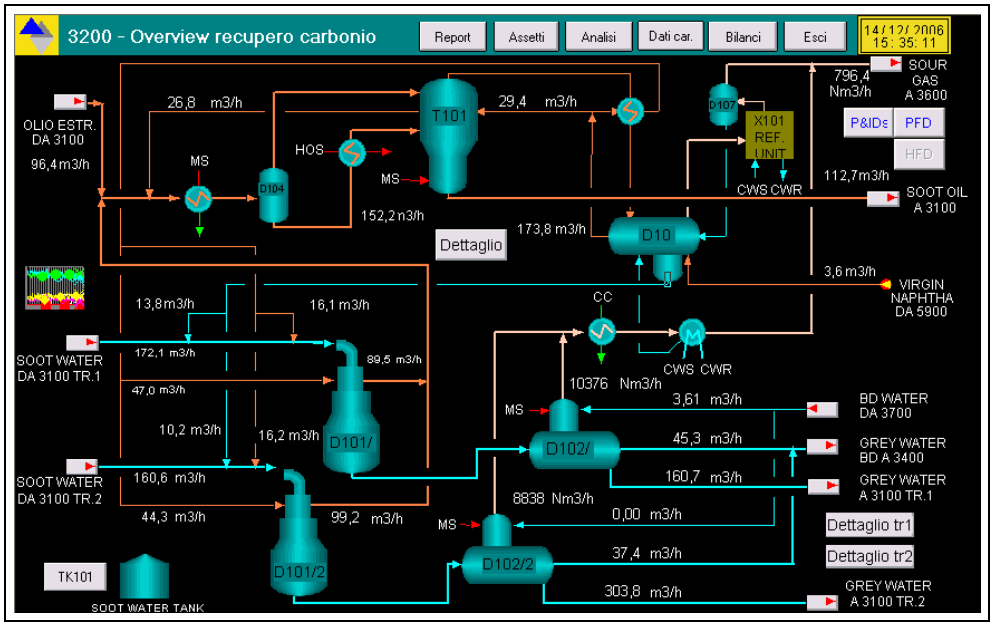

Figure 3. Hardcopy of a part of IGCC plant DCS

This is the base for carrying out an interaction between the DCS and the Fault Tree Analysis.

OLFTA system continuously receives from the DCS information about the equipment state (both not running and out of operative range are considered failures) and then it recalculates the probability of the top event in order to take into account of the current faults.

In order to obtain this result, the OLFTA Main Page was realized using a Microsoft Excel© worksheet, as shown in Figure 4, by which it is possible to assess the occurrence probability of the Top Event, calculated for a variable mission time (t_M).

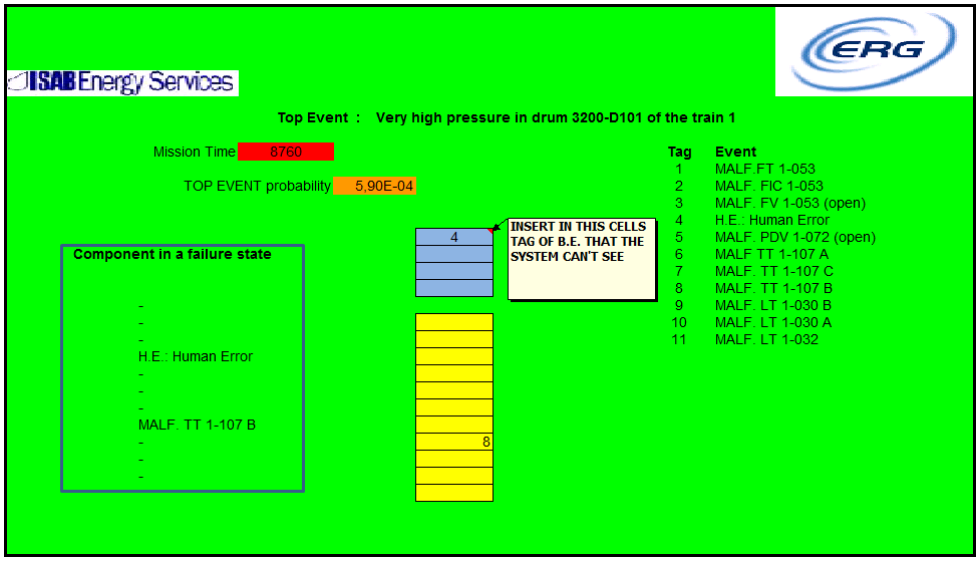

Figure 4. OLFTA Worksheet main page

The information coming from the DCS regarding equipment failures is automatically recorded also in the worksheet; a list of components in a failure state appears on the left side of the screen and the probability of the Top Event is recalculated, taking into account of the occurred events, and spotted in the same page.

If there are some basic events that the system can't see (i.e. human errors or failure states of equipment not automatically controlled) it is possible to input a number of this basic event in the specific cells, in order to take into account also of these failures to assess the potential occurrence of the Top Event.

A particular attention was devoted to the common cause failures in order to avoid that a failure which involves more than one equipment was considered more than one times. A specific worksheet is used in order to highlight the common cause failures and its results are linked to the main page.

Another very important function of the OLFTA software is the possibility of printing, in a new worksheet, the current fault tree, as shown in Figure 5. This is a very useful function because it allows to have a global view of the state of each top event causes (basic events).

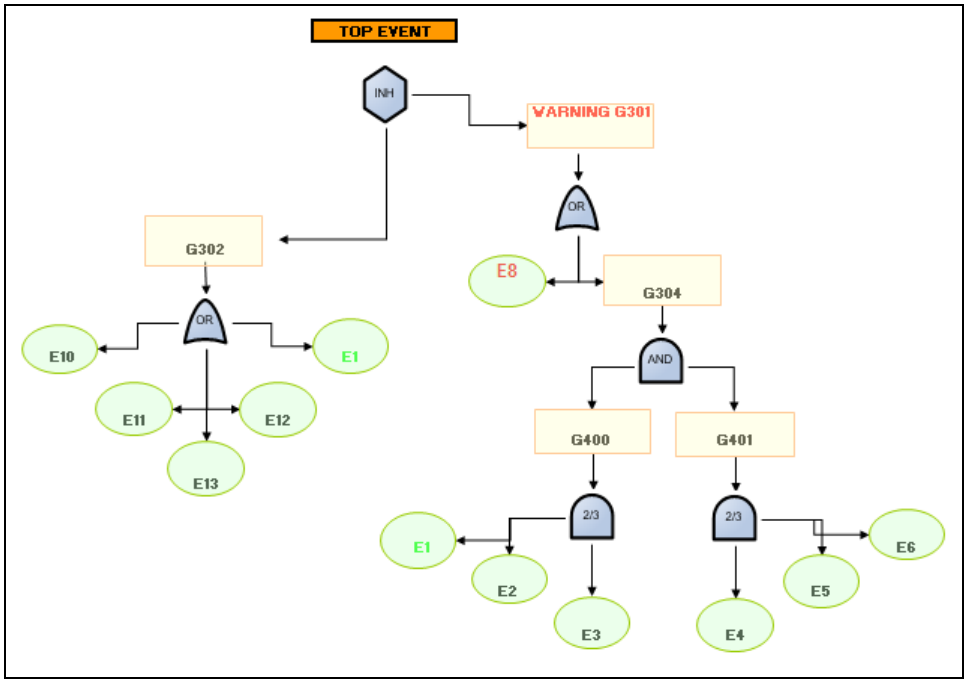

Figure 5. OLFTA Example

If the text color of the basic event is black the equipment is correctly running; if the text color is green the event is a common cause event (still functioning, as for the event E1 in Figure 5); if some basic event is occurring the text color becomes red (as for the event E8 in Figure 5), so that it is possible to see where the failure happened and if there are enough safeguards to avoid the Top Event occurrence. When an event occurrence can generate a failure in an higher level event a warning signal is shown in the Fault Tree (as is "warning G301" generated by the E8 failure in Figure 5).

4.1 OLFTA probability calculation and comparison with static FTA

Results obtained by this software application allow to see how the breakdown of a single instrumentation can change the occurrence of the Event Top in a significant way.

To show the influence of different equipment we introduce two examples:

1. the transmitter FT1_053 is broken;

2. PDV1_072 fails.

If we consider the previous example, we can see that the instantaneous unavailability of the Top Event is 7,52*E-05; when the transmitter FT1_053 is broken, the Top Event instantaneous unavailability becomes 5,90*E-04; moreover if the pressure valve PDV1_072 fails the instantaneous unavailability will be 1.

This is the correct way to assess the Birnbaum's Importance Measure IBi(t) that is the probability that the *i*-th component was critical to the functioning of the system at time t. This index can help the safety and maintenance engineering in defining activities based on risk priority. In the previous example the OLFTA software allows to understand that it was mandatory to double the PDV valve.

In order to validate the system, the output of the OLFTA software was compared with other software packages commonly used by risk-analysts (ASTRA FTA) and no significant difference was pointed out, as shown in Table 6 (the TE probability values are in the same order of magnitude).

Table 6. Comparison of static FTA results with OLFTA and ASTRA FTA

Description	On-Line FTA	Astra FTA
Very high pressure in D101	7,98*E-06	8,89*E-06
Very high pressure in D102	2,40*E-05	1,61*E-05
Very high temperature in R101	2,40*E-07	2,31*E-07
P101 Pump cavitation and flammable product loss from seal	2,41*E-08	1,24*E-08
High pressure in D111	1,62*E-08	2,11*E-08
High pressure in stripping column T104	5,42*E-08	5,42*E-08
High pressure in stripping column T103	3,69*E-12	7,30*E-12
High pressure in D112	3,92*E-13	4,51*E-13
High pressure in D103	2,81*E-07	6,92*E-07

5.0 CONCLUSIONS AND FUTURE DEVELOPMENT

The OLFTA software allows an FTA to become an instrument which let us to know the effective "health" of the plant in real time and let us to know if the industrial plant is in a critical situation for the considered Top Event.

The historical failure data of the equipment were also useful to correlate the Top Event probability to the failure significant events, in order to assess the criticality of each failure event and to avoid recurrent failures.

The choice of using a simple worksheet to report the failure or the operative state of an equipment was appreciated by the Company for its simplicity in use and for the little implementation costs.

A future development could be the implementation of a Condition Based FTA which allows to overcome the limit of FTA concerning the constant failure rates (accidental failures), considering also the deterioration processes [12]; this can allow to the safety and maintenance engineers to monitor the residual life of each equipment.

REFERENCES

[1] Italian Legislative Decree 238/2005, Transposition of Directive 2003/105/EC of the European Parliament and of the Council of 16 December 2003 amending Council Directive 96/82/EC on the control of major-accident hazards involving dangerous substances.

[2] Italian Legislative Decree 334/1999, Transposition of Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances.

[3] Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances, EU Official Journal L 010, 14/01/1997, p. 0013 – 0033.

[4] Sullivan, K.J., Dugan, J.B. and Coppit D., The Galileo fault tree analysis tool, Proceedings of the 29th Annual International Symposium on Fault-Tolerant Computing, Madison, USA, 15-18 June 1999, pp. 232-235.

[5] Dugan, J.B., Venkataraman, B. and Gulati, R., DIFtree: a software package for the analysis of dynamic fault tree models, Proceedings of the Reliability and Maintainability Symposium, Philadelphia, USA, 13-16 January 1997, pp. 64-70.

[6] Cepin, M. and Mavko, B., A dynamic fault tree, Reliability Engineering and System Safety, 75, 2002, pp. 83-91.

[7] Dugan, J.B., Sullivan, K.J. and Coppit, D., Developing a low-cost high-quality software tool for dynamic fault-tree analysis, IEEE Transactions on Reliability, 49, No. 1, 2000, pp. 49-59.

[8] Manian, R., Coppit, D.W., Sullivan, K.J. and Dugan, J.B., Bridging the gap between systems and dynamic fault tree models, Proceedings of Annual Reliability and Maintainability Symposium, Washington DC, USA, 18-21 January 1999, pp. 105-111.

[9] Birolini, A., Reliability Engineering. Theory and Practice, 2007, Springer.

[10] Roberts, N.H., Vesely, W.E., Haasl, D.F. and Goldberg, F.F., Fault Tree Handbook, 1981, NUREG-0492, Washington.

[11] ASTRA, Advanced Software Tool for Reliability Analysis, Version 3.0, European Commission, Joint Research Centre, Ispra (VA), Italy.

[12] Shalev, D.M. and Tiran, J., Condition-based fault tree analysis (CBFTA): A new method for improved fault tree analysis (FTA), reliability and safety calculations, Reliability Engineering and System Safety, 92, 2007, pp. 1231–1241.